

A simple guide to Computer Viruses and other dangerous little programs

An Introduction to an Effective Defense



Roberto Dillon, Ph.D.

About the Author

Roberto Dillon was born in Genoa, Italy, in 1973.

In 1981 he had his first encounter with a home computer, a Texas Instrument 99/4A, and in 1983 he received a Commodore 64 that hooked him into technology and computer science ever since.

Roberto holds a Master and a Ph.D. degree in Electrical and Computer Engineering from the University of Genoa (both his thesis focused on computational models for analyzing emotions in music playing with applications to interactive media) and worked as Programmer / Analyst in his hometown before moving to Stockholm, Sweden, as a Guest Researcher at the department of Speech, Music and Hearing within the Royal Institute of Technology (KTH).

In 2005 he moved to Singapore as a Research Fellow at gameLAB in Nanyang Technological University for designing and developing innovative and educational computer games, with a special focus on artificial intelligence and interactive audio techniques.

Since 2007 he moved to the “School of Interactive and Digital Media” at Nanyang Polytechnic, still in Singapore, where he is lecturing the "Audio Creation" module (i.e. sound design and programming for games) besides being involved in the school’s game development activities.

His main project so far, the ‘Virtual Orchestra’, an original game/simulation for introducing children to music, was featured internationally on newspapers and magazines such as ‘The Straits Times’ (Singapore), ‘The Taipei Times’ (Taiwan), MUSO (UK) and ‘USA Today’ where it was introduced as the ‘guitar hero for the symphony crowd’.

He is an IGDA (International Game Developers Association) member and can be reached via email at roberto.dillon@member.igda.org

Copyright notice

All logos and program screenshots are properties of their respective owners and are shown for the sole purpose of identifying the various companies and products that the ebook is describing.

A limited number of screenshots of the products described is believed to qualify as fair use of the material, as such display promotes the particular product and its authors and does not impede the rights of the copyright holder in any way.

The cover picture is copyrighted by Elisa Marchi.

Roberto Dillon © 2007

Contents

Introduction	4
What are Computer Viruses?	5
What is Spyware?	8
Worms? Trojan Horses??	10
Help! My Browser was Hijacked!	12
The next target....	13
To know more	14

Introduction

Welcome!

Thanks for downloading this little ebook which I tried to pack with as much useful information as possible.

Computer malware has been a serious issue for many years and, unfortunately, it's very likely to stay with us for a long time to come. Anyway, we have many tools at our disposal, including excellent free ones, for arranging an effective defense and this guide will introduce you to the various dangers you might face in future together with easy methods for getting rid of them and restore your computer an healthy status.

Each of the main malware categories (viruses, spyware/adware, worms/trojan horses, browser hijackers) are faced one by one by explaining what they do and then by answering to simple questions in a plain F.A.Q. style. For example, "Where and how can I get infected?", "How can I defend?" are the kind of Q&A you'll find throughout the book.

I hope you will find the information and programs presented useful and I wish you good luck in getting rid of these annoying and very dangerous computer threats.

Roberto Dillon

Singapore, 15th June 2007

What are Computer Viruses?

Melissa, I love you.... This could be the beginning of a sweet love letter but, instead, to many computer users, it will remind of two terrible viruses that in 1999 and 2000 affected countless machines all around the world.

But what are computer viruses exactly? And where they come from?

The term is nowadays used to commonly identify all types of ‘malware’ (a generic term for indicating all those programs that you’d not like to run on your computer but somebody else wants to), including those that will be introduced in the next chapters. Anyway, proper ‘Computer Viruses’ are defined as small programs that are able to find a way to execute and propagate themselves without the explicit consent of the host computer’s owner for performing tasks that, very often, have a direct damaging effect on the host machine. Once this is accomplished, they also have to find a way to propagate themselves to infect other computers.

Viruses had their first appearance in the early eighties as simple jokes or even as a tool to protect original software by identifying and destroying pirated copies. In those days they had a limited diffusion since they could only spread by removable media such as floppy disks or tapes and so couldn’t do much harm on a larger scale. Things changed drastically with the birth of BBS (bulletin board systems, where computer users traded programs and often pirated games) and then with the spread of the Internet and email messages: these new resources gave many people the possibility to damage enemies or large corporations (by deleting files, formatting hard disks or making computers unstable and impossible to use) for political or other reasons or for trying to steal sensible data (like passwords, credit card numbers etc.) from other users.

Many different types of viruses exist. Let’s have a look at the most common:

- **Boot virus:** this is a kind of virus that hides in the boot sector of a floppy or hard disk so as to be executed as soon as the computer starts or the floppy is inserted. These kind of viruses were common years ago when the viruses had to propagate through removable media such as the floppy disks.
- **Companion virus:** usually viruses get attached to another program to be executed whenever the legitimate software is run by the user. This kind of virus, popular during the DOS days, instead tried to trick the user by creating new executable files with the same name of tools and commands of common use but with a .COM extension instead of the .EXE typical of the “real” file. When, from the command prompt, the user typed the name of the command to execute (without specifying the extension), the OS chose to execute the name coming first in alphabetical order, i.e. the virus that named itself with the .COM suffix instead of the legitimate .EXE one.

- **E-mail virus:** this is one of the most common kinds of viruses since the late nineties thanks to the Internet (Melissa and 'I love you' belonged to this category). The virus simply travels through an email message and disguise itself as a captivating attachment which needs to be executed by the email recipient. Once activated, the virus gets control of the machine and can, for example, replicate itself to all the user's email contacts.
- **Macro virus:** this type of virus usually targets Microsoft Office applications like Word and Excel, which can execute small programs to enhance particular functions. Usually they can't do much physical harm to the machine but they can, for example, check and record whatever we are typing (which is, of course, very dangerous).
- **Cross site scripting virus (XSSV):** a relatively new kind of virus (detected in 2005) that spreads through infected web pages by exploiting web browser vulnerabilities.

So, how can we understand whether we have been infected by one of these viruses? It shouldn't be too difficult: most viruses, soon or later, will show their malicious effects: if some type of files (like mp3 or jpg images) are suddenly missing, if we are receiving angry emails from unknown people who are complaining we are spamming them, if our trusted machine, equipped with the latest processor, starts going as slow as an old 286 or if it starts rebooting itself without any reason, well, there are good chances we have been infected and we should take immediate action, but don't worry: we are going to introduce some free effective tools that will allow you to sleep without worries (though keeping an eye open is always a good practice! ;-))

In summary:

Where and how can I get infected by a virus?

Usually by opening email attachments but also by using infected Word/Excel files, floppy disks or even by surfing the internet.

How can I defend?

First and foremost, install an updated antivirus (only one: more antivirus together can interfere with each other!). Besides the most common and widely trusted commercial ones, also free but very reliable programs exist.

Personally, I found very useful the following couple of products:

Avast! - Home Edition: an antivirus by Alwil Software, on the scene since 1988. This product is very user friendly and allows for fast and automatic updates. It scans all incoming and outgoing emails and offers real time protection against many types of malware. A code is needed for completing the free registration (for personal use only) and, after one year, the user is required to get a new free code to renew the updating



subscription.

Download the latest version from <http://www.avast.com>

Avira AntiVir – Personal Edition: a winner of several awards which is used by more than 15 million users worldwide and detects more than 80,000 viruses. It is also able to check for other malware such as Worms and Trojan Horses and allows to schedule scans and update checks at fixed time intervals.

You can download it from <http://www.free-av.com/>



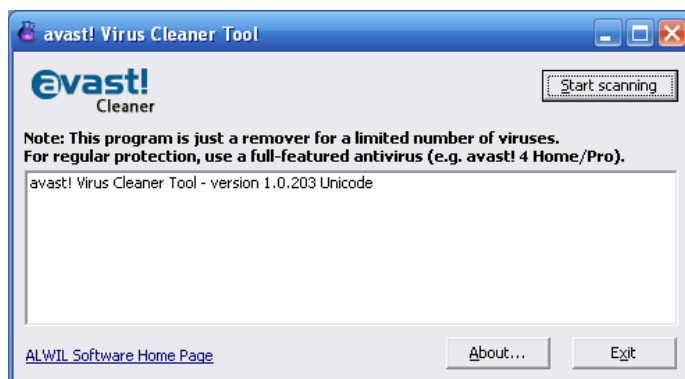
Help! I have been infected! What should I do?

Ok, don't panic! Once the antivirus detects 'something' in the system, it will usually try to remove it or to isolate it so that it can make no harm. Anyway, it may not always succeed (unfortunately it may be impossible to remove the virus once it's active in the system) so other options will have to be considered.

Specific free "virus removal" tools are available to target the most common and widespread kind of infections, for example:

Avast Virus Cleaner:

Get it from <http://www.avast.com/eng/avast-virus-cleaner.html>



Avast! Virus cleaner ready to start scanning

VCleaner from AVG Antivirus:

Get it from <http://www.grisoft.com/doc/112/lng/us/tpl/tpl01>

Remember that, when running a virus removal tool, it's usually a good idea to start the computer in "safe" mode to prevent the virus to get a chance of activating itself during the standard system startup (on Windows XP, press F8 during the computer boot and select the proper option in the booting menu that will appear).

If everything fails, it may be needed to restore a previous (clean!) system configuration through the Windows System Restore option (on Windows XP, right click on 'My Computer', select Properties and then the 'System Restore' tab).

AVG Free AntiSpyware: from GriSoft (a well known software house that also releases a free, though limited, version of their excellent AVG antivirus software for home use, both for Windows and Linux. If interested, check <http://free.grisoft.com/doc/1>). This is an easy to use tool that incorporates also heuristic techniques to identify unknown threats.

You can download it from:

<http://free.grisoft.com/doc/avg-anti-spyware-free/lng/us/tpl/v5>

Good prevention habits:

Besides having an anti-spyware tool such those described in the previous section, we should always surf the internet with at least moderate attention: whenever we face some apparently interesting but unknown software tool or a webpage that offers amazing little utilities or even prize-winning opportunities, we should think twice before doing anything. In fact, some spyware are also installed through apparently innocuous pop-up window where clicking 'ok' or even 'cancel' will actually trigger a program that will "infect" our web browser and then spy our behavior. For this reason, it's always a good habit to close such unwanted windows by clicking on the 'x' at the top right corner instead of clicking on the 'Cancel' button.

We should download only content from sources we trust and, for an effective prevention, it's very important we set proper browser security settings otherwise malicious downloads could even start automatically! To do this, in Internet Explorer, open the Tools menu, 'Internet Options' and select the 'Security' tab. Choose at least Medium security level (of course High could be a better choice though it would block also honest content) or, if you know what you are doing, select 'custom level' and turn off the options you consider dangerous (usually, this means at least selecting the 'prompting' option before installing/running any ActiveX component).

In any case, since many kind of spyware are always constantly trying to infiltrate in our computer, it's a wise habit to regularly scan our system with a trusted anti-spyware tool and check that everything is in order.

Worms? Trojan Horses??

Unfortunately malware programs don't limit themselves to viruses or spyware/adware but include also other categories that we should consider and watch out for.

It's interesting to know that the first 'worm' is even older than the first officially known virus. It was programmed in 1978 by two researchers at Xerox (John F Shoch and John A Hupp) with the aim of finding idle processors on a network and assigning them some useful tasks.

The term 'worms' in fact describes a program which is able to replicate itself and spread across a network looking for possible targets without any user intervention and without the need of attaching itself to some other program like a virus does.

On average, worms are relatively harmless for the single user: they just propagate themselves with the only consequence of slowing down the network (eventually, they can make it collapse) but they don't try to directly damage the system by deleting files, for example.

More devilish worms exist, though. Some types can in fact open a 'backdoor' into the computer which can then be used by a hacker for illegal activities (like spamming or file transfer purposes).

Where and how can I get infected by a worm?

Worms can propagate in several different ways, including emails, instant messaging and chat rooms (by sending links to infected websites) and straight through the internet by looking for vulnerable systems. The latter is probably the most dangerous threat since in this way worms can infect and propagate through computers at an extremely fast rate: in fact, if we leave a computer connected to the internet without any kind of protection, it's just a matter of seconds before some worm finds it and infects it!

How can I defend?

While in a chat room or in an instant messaging session, think twice before clicking on some unknown link that popped out from nowhere.

Regarding Internet worms, they tend to exploit system vulnerabilities so it's always very important to keep Windows (or any other OS) up to date by downloading and installing all available security patches (Windows XP can do this automatically: check the "Automatic updates" tab in the "System properties" by right clicking on your "My computer" icon).

Antivirus and spyware programs also check for worms and provide a good defence.

Another step is to activate a firewall so as to monitor and block intruders who look for open ports in our system. Windows XP comes with its own firewall (check the "Control Panel") but good freeware firewalls are also available:

Outpost Personal Firewall:

<http://www.agnitum.com/products/outpostfree/index.php>



Zone Alarm Free (non-business use):

http://www.zonelabs.com/store/content/company/products/trial_zaFamily/trial_zaFamily.jsp?lid=home_freedownloads

Let's talk about Trojan Horses now.

Trojan horses are programs that look useful but instead are (or contain) something which aims at damaging the user. For example, the type of spyware that we met in the previous chapter that tries to trick the user for being installed by making him believe they are something useful, can also be classified under the "Trojan horses" category.

There are many different types of Trojan horses that, once activated by our installation, can do any kind of damage to our system: deleting files, drop other viruses, record what we are doing, send spam, open backdoors in our computer (like worms), restart our system or just do silly things like opening and closing the CD-Rom tray.

Where and how can I get infected by a trojan horse?

Due to their cheating nature, Trojan horses are commonly spread through websites as free software downloads, through email attachments or as 'rare' songs in P2P networks.

How can I defend?

First of all, set your antivirus to automatically scan incoming emails, then don't download freebies from unknown sites (and don't look for copyrighted material in P2P networks! ;-)

Besides these commonsense rules, a firewall is also good to have to check whether unknown programs are trying to open a port in our system to send/receive sensible data.

If so, we have the proof we have been infected.... But no need to worry: just read the next paragraph!

Help! I have been infected! What should I do?

This is an effective free malware scanner that looks and removes Trojan horses, worms and other nasty things: <http://www.emsisoft.com/en/software/free/>



Help! My browser was hijacked!

If your browser suddenly decides to go where it wants, to start from an unknown page, to direct your searches on weird engines, to add new sites of dubious nature into your favorites or to launch many popup windows.... Well, it's a clear sign there is something wrong running on. More precisely, you have been hijacked!

Where and how can I get infected?

Clearly by surfing the internet. This sort of malware is often found lurking for victims within porn or hacker/warez sites.

Usually, these programs are ActiveX controls that succeed to automatically launch themselves if the browser security settings are low enough. Some scripts are even so smart and evil to find and exploit always new Internet Explorer vulnerabilities to launch themselves regardless of the browser's security settings!

How can I defend?

Keep your browser updated by checking for new security packages: assuming you are using Internet Explorer, these are usually downloaded automatically along with Windows updates (we saw how to do this in page 8).

Avoid dangerous sites and use a browser which works in a different way from IE (like Firefox or Opera) since most hijackers use to target Microsoft's product.

Help! I have been infected! What should I do?

Unfortunately simply changing back the browser settings to meaningful values doesn't work (unless we were very lucky and met a very harmless kind of hijacker!) since the program that altered our system very likely has also saved its values inside the system registry to keep setting them as it wishes.

A good move is to reboot and start the system in safe mode (to block the malicious scripts before they can start themselves and eventually block us from removing them) then scan the system with either Spybot or Ad-Aware. In fact these two software, which we introduced in page 6, also look for this kind of malware.

If they are not able to fix the problem, then it's high time to start playing tough and take one of these two utilities: HijackThis

<http://www.snapfiles.com/get/hijackthis.html>

and CWShredder

<http://www.trendmicro.com/cwshredder/>

These programs have the ability to scan the system and identify suspicious elements giving us the chance to remove them once and for all.



CWShredder ready to scan

The next target....

Unfortunately, home computers aren't the only target for malware programs. There are some common devices which are getting smarter and more powerful everyday, featuring more and more complex operating systems.... If you are thinking I'm talking about mobile phones, you are right!

Recently some viruses designed to hit (mostly) Windows Mobile platforms have been spotted and they are likely to grow in number and capabilities in a near future.

Where and how can I get infected?

So far, these programs are usually transmitted as ringing tones or images/MMS

How can I defend?

Simply put, don't open images or tones coming from unknown people or downloaded from unreliable sites!

In any case, several companies are developing antivirus programs to run on mobile systems. These are commercial products but trial versions are usually available for download.

Among the available products, we have "Symantec AntiVirus for Handhelds Corporate Edition" (available for Win Mobile and PalmOS, for more information check http://www.symantec.com/home_homeoffice/products/overview.jsp?pcid=pf&pvid=savhh), AhnLab's "Symbian OS V3" antivirus (for Symbian smart phones) and also products from F-Secure (trial version downloadable here: <http://mobile.f-secure.com/downloads/trial/index.html>) and BullGuard (for Win Mobile and Symbian. More information at <http://www.bullguard.com/mobile/>).

Two smart phones running BullGuard antivirus



To know more

The Wikipedia, a free community-created online encyclopedia, is always a good place to start in depth searches on any topic, computer malware included.

Some useful pages are the following:

http://en.wikipedia.org/wiki/Computer_virus

http://en.wikipedia.org/wiki/Computer_worm

http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29

<http://en.wikipedia.org/wiki/Adware>

<http://en.wikipedia.org/wiki/Spyware>

If you want to know more about one of the latest virus threats, the so called “cross site scripting viruses”, it’s worth having a look at:

<http://www.bindshell.net/papers/xssv>